UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

CORNELIUS ALLISON, on behalf of himself and all others similarly situated,	:	Civil Action No. 09-cv-2560-LDD
Plaintiff,	:	JURY TRIAL DEMANDED
v.	:	
AETNA, INC.	:	
Defendant.	:	

AMENDED CLASS ACTION COMPLAINT

Plaintiff Cornelius Allison ("Plaintiff") brings this class action suit against Aetna, Inc. ("Aetna" or the "Company"). Plaintiff makes the following allegations, except as to allegations specifically pertaining to Plaintiff and Plaintiff's counsel, based upon the investigation undertaken by Plaintiff's counsel, which included, *inter alia*, review and analysis of Defendant's website, various other websites, various news articles, and correspondence from Aetna to affected individuals. In support of Plaintiff's Amended Class Action Complaint ("Complaint"), Plaintiff alleges as follows:

JURISDICTION & VENUE

1. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because some Class members are of diverse citizenship from Defendant; there are more than 100 Class members nationwide; and the aggregate amount in controversy exceeds $5,000,000. This Court has personal jurisdiction over the parties because

Defendant is incorporated in Pennsylvania, maintains offices in this state, and conducts business here.

2. Pursuant to 28 U.S.C. § 1391(a)(2), venue is proper in the Eastern District of Pennsylvania because a substantial part of the acts giving rise to Plaintiff's claims, such as the transactions by which Defendant became privy to Plaintiff's Sensitive Information (as hereinafter defined), occurred in this District.

NATURE OF ACTION

3. This is a class action lawsuit brought on behalf of Plaintiff and all other persons similarly situated against Aetna for its failure to adequately protect the private personal information of its current, former, and potential employees, including but not limited to their email addresses, names, Social Security numbers, home and/or office addresses, telephone numbers, employment histories, and other information ("Sensitive Information").

4. Class members were required to input their Sensitive Information into Aetna's website when they applied for a job with Aetna. Aetna also stored current and former employees' Sensitive Information on its website.

5. Aetna unlawfully failed to maintain reasonable systems and procedures to protect Plaintiff's and the Class' Sensitive Information. As reported on May 27, 2009, as a result of Aetna's inadequate data security system, Aetna's website was hacked into by unknown third parties, and Class members' Sensitive Information was accessed and/or misused by unauthorized persons.

6. Aetna's website contained Sensitive Information of over 450,000 individuals.

7. Plaintiff seeks damages suffered as a result of Defendant's practices, including

but not limited to compensatory damages and injunctive relief.

PARTIES

8. Plaintiff Cornelius Allison is a resident of Darby, Pennsylvania. As described further below, Plaintiff previously worked for Aetna from December 1998 through May 2005. Then, in January 2009, he applied for another position at Aetna, whereby he input his personal information into Aetna's website. In May 2009, he received a letter from Aetna stating that his personal information had been accessed by an unauthorized person. He misplaced the letter and requested a second letter from Aetna. Aetna sent him a replacement letter dated July 16, 2009. A copy is attached hereto as Exhibit 1.

9. Defendant Aetna, Inc. is a Pennsylvania corporation with its principal place of business located in Hartford, Connecticut. Aetna is a diversified healthcare benefits company that provides healthcare and related benefits, serving healthcare members, dental members, and group insurance customers. The Company offers medical, pharmacy, dental, behavioral health, group life and disability plans, and medical management capabilities and health care management services for Medicaid plans.

FACTUAL BACKGROUND

Security Breaches Lead to Identity Theft

10. By way of background, the United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves can use identifying data such as Social Security numbers to open financial accounts and incur charges

and credit in a person's name.[1] As the GAO has stated, this type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating.

11. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

12. According to the Federal Trade Commission ("FTC"), identity theft victims must spend countless hours and money repairing damage to their good name and credit record.[2] Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. In addition, a person whose personal information has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

13. Identity theft crimes often include more than just crimes of financial loss. Identity thieves also commit various types of government fraud, such as: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security number to obtain government benefits; or filing a fraudulent tax return

[1] *See* http:///www.gao.gov/new.items/d07737.pdf.

[2] *See* FTC Identity Theft Site, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/

using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

Aetna's Privacy Policy

14. Aetna represented to Plaintiff and the Class that it will protect their Sensitive Information. On Aetna's website, where it requested that job applicants provide their personal information, Aetna stated: "All information will be held in the strictest confidence."

15. The job application website also has a section titled "Web Privacy Statement" stating:

> Any nonpublic personal information that you may provide via our sites will be used solely for the purpose stated on the page where it is collected. . . . Aetna will not sell, license, transmit or disclose this information outside of Aetna and its affiliated companies unless (a) expressly authorized by you, (b) necessary to enable Aetna contractors or agents to perform certain functions for us, or (c) required or permitted by law. In all cases, we will disclose the information consistent with applicable laws and regulations and we will require the recipient to protect the information and use it only for the purpose it was provided.

16. The Web Privacy Statement contains a subheading titled "Security" stating:

> Aetna has adopted and adheres to stringent security standards designed to protect non-public personal information at aetna.com against accidental or unauthorized access or disclosure. Among the safeguards that Aetna has developed for this site are administrative, physical and technical barriers that together form a protective firewall around the information stored at this site. We periodically subject our site to simulated intrusion tests and have developed comprehensive disaster recovery plans.

---

about-identity-theft.html.

17. These representations are collectively referenced herein as Aetna's "Privacy Policy."

The Data Breach at Aetna

18. On or around May 27, 2009, Aetna publicly announced that its job application website was accessed by unauthorized persons.

19. As reported by the Associated Press that day, Aetna's website held email addresses for approximately 450,000 people who applied for jobs or submitted resumes to the Company. Aetna stated that Social Security numbers of current and former employees and people who received job offers were stored on the website. For people who received job offers, the website also stored phone numbers, addresses, and employment histories.

20. Aetna's spokesperson Cynthia Michener is quoted as saying: "We know for certain that the emails were accessed, we don't know whether or not anything else was accessed." Michener said that some emails were copied from the website and then used by the hackers to contact job applicants.

21. Aetna reportedly found out about the breach in early May 2009 when people complained to the Company that they received spam ("phishing") email messages that appeared to come from Aetna. The spam purported to be a response to a job inquiry and requested more personal information.

Aetna Urged Class Members to Take Steps to Avoid Identity Theft

22. In late May 2009, Aetna contacted approximately 65,000 current and former employees whose Social Security numbers were at risk. Aetna stated that there had been a

security breach of Aetna's website, and that current and former employees' Sensitive Information had been compromised. The letter also advised recipients to monitor their personal accounts for fraudulent charges, and to place fraud alerts on their credit files. The letter also stated that Aetna would provide recipients with one year of free credit monitoring. The letter stated the following, in relevant part:

> We recently learned that e-mail addresses were accessed from a web site and database . . . [used] to manage job applications for current or previous Aetna employees. Because other personal information about current or previous Aetna employees is included in this same database, it is possible that other personal information may have been exposed. . . .
>
> While we are not able to verify whether your personal information was accessed, the database included information you provided as an employee with Aetna. This information included your name, address, Social Security Number (SSN), date of birth, phone number, e-mail address and information pertaining to prior jobs. . . .

23. Aetna's letter contained an attachment urging recipients to take various measures to prevent identity theft. The attachment stated, in relevant part:

> We urge you to monitor your personal accounts (e.g., bank statements, credit card bills, etc.) for charges or other items you do not recognize.
>
> We also urge you to place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. . . .
>
> . . . .
>
> [R]eview [your credit report] carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security Number, address(es), complete name and employer(s). . . .

Class Members Spent Time and Money Responding to the Breach

24. Class members had to expend considerable time and effort as a result of the data

breach. For example, Plaintiff and Class members had to perform various time consuming tasks, including but not limited to reviewing banks statements, credit card bills, and credit reports for fraud, requesting credit reports and fraud alerts from credit reporting agencies, and signing up for credit monitoring.

25. Moreover, fraud alerts (urged by Aetna) are an inconvenience to consumers because fraud alerts delay and complicate the process of opening legitimate new sources of credit.

26. In addition, many Class members, like Plaintiff, incurred out-of-pocket costs for identity theft protection services and other items as a result of Aetna's actions.

27. The time and effort expended, inconvenience experienced, and out-of-pocket costs incurred by Class members constitute actionable damages. They are also necessary steps aimed at mitigating damages from identity theft.

28. Class members face a significant risk of identity theft, evidenced by:

a. The hackers' efforts to extract personal information from Class members via sending phishing email messages. Hackers would not seek such information if they did not intend to misuse it.

b. Aetna's offer of free credit monitoring. Aetna would not offer credit monitoring if identity theft was not a significant risk.

c. Aetna's instructions to Class members to take numerous burdensome steps to protect themselves from identity theft. Aetna would not recommend these steps if identity theft was not a significant risk.

29. In light of the identity theft risk, Class members spent time and money responding

to the breach.

30. The Restatement (Second) of Torts § 919(1) states: "One whose legally protected interests have been endangered by the tortious conduct of another is entitled to recover for expenditures reasonably made or harm suffered in a reasonable effort to avert the harm threatened." Aetna's wrongful conduct endangered Class members' legally protected interests in data privacy. Class members are entitled to recover for their time and money spent as a result of the data breach and in an effort to avert identity theft.

31. Aetna's offer of one year of free credit monitoring is insufficient. Class members need protection for more than one year. As noted above, fraudulent use of identifying information often lasts much longer than one year.

Aetna's Wrongful Conduct

32. Aetna knew or should have known that its website for processing and storing Class members' job applications was not secure.

33. Aetna's security failures included, but are not limited to, the following:

a. Failing to maintain an adequate data security system to prevent intrusion;

b. Unjustifiably retaining Sensitive Information on its computer system for years;

c. Failing to align data security processes with internal policies;

d. Failing to mitigate the risks of a data breach;

e. Using an unsecured website to collect applicants' Sensitive Information; and

f. Failing to encrypt Sensitive Information of applicants and employees.

34. Aetna learned of the breach in early May 2009 or sooner. However, Aetna did

not notify affected individuals until late May 2009. No reason has been given by Aetna for its delay of at least several weeks in providing notice.

35. Although Aetna sent notification letters to 65,000 current and former employees, it did not contact the remainder of the 450,000 individuals (job applicants) to notify them of the breach. No reason has been given by Aetna for not notifying the latter group.

36. Significantly, Aetna had previously experienced another data breach in 2006, when an employee's laptop was stolen. Over 38,000 persons were affected in that breach. Thus, Aetna was aware of the need for strict security protection over personal data, and the consequences that could result from a data breach.

Plaintiff Allison

37. Plaintiff Allison was employed at Aetna as an office assistant from December 1998 to May 2005. He worked in Aetna's office located in Blue Bell, Pennsylvania.

38. In January 2009, Plaintiff Allison used Aetna's website to apply for a customer service position. As required by Aetna, he input his personal information and uploaded his resume onto Aetna's website.

39. In May 2009, Plaintiff Allison received a letter from Aetna advising him of the data breach. He misplaced the letter and received a replacement letter dated July 16, 2009. *See* Exhibit 1.

40. In response to the letters, Plaintiff Allison tried to log onto his bank's website to review his account activity. He was unsuccessful. He then drove to the bank and obtained copies of his bank statements from January 2009 through June 2009. He reviewed the statements for fraud. This was time-consuming and burdensome.

41. Plaintiff Allison signed up for Aetna's offer of one year of free credit monitoring.

42. Plaintiff Allison purchased an identity theft protection service called IDFreeze from TrustedID. He pays $10.00 per month for the service. According to IDFreeze's website, "IDFreeze is different from credit monitoring services which only alert you after there is a problem. IDFreeze helps stop identity theft before it happens and protects you well beyond what credit monitoring can offer." IDFreeze provides the following benefits, among others:

a. Public Database Scanning: "We monitor hundreds of public record databases that contain information about everything from your marital status and address to issues of the court and business applications. If we detect anything that looks unusual and could lead to identity theft, we'll alert you immediately."

b. Black Market Scanning: IDFreeze will "regularly patrol the black market Internet where identity thieves buy and sell" stolen information for evidence of a client's Social Security number, credit card numbers, bank account numbers, and name and address. If a client's information is discovered, IDFreeze will notify the client immediately.

c. Medical Benefits Protection: "One of the newest and most dangerous forms of identity theft is medical benefit fraud. We'll help you review your medical benefit statements to ensure that you and your family are the only ones being treated with your medical benefits."

43. In sum, Plaintiff Allison has incurred out of pocket costs as a result of the data breach. He also spent several hours responding to the breach and attempting to mitigate his risk. The time spent included, among other things, researching the breach, traveling to and from his

bank, obtaining and reviewing bank statements, signing up for Aetna's credit monitoring offer, signing up for the IDFreeze identity theft protection service, and reviewing correspondence from the credit monitoring company and IDFreeze.

CLASS ACTION ALLEGATIONS

44. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this class action individually and on behalf of all other persons whose Sensitive Information was accessed from Aetna's job application website by unauthorized persons (the "Class"). The Class does not include Defendant, or its officers or directors.

45. On information and belief, the Class is compromised of hundreds of thousands of persons, making joinder of such cases impracticable. Disposition of the claims in a class action will provide substantial benefits to the parties and the Court.

46. The rights of each Class member were violated in a similar fashion based upon Defendant's uniform actions. Some common issues present here are:

a. Whether Defendant was negligent in collecting and storing Plaintiff's and Class members' Sensitive Information;

b. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class members' Sensitive Information;

c. Whether Defendant breached its duty to exercise reasonable care in storing Plaintiff's and Class members' Sensitive Information by storing that information on its computer systems in the manner in which it did;

d. Whether implied or express contracts existed between Defendant and Class members;

e. Whether Plaintiff and the Class are at an increased risk of identity theft or other malfeasance as a result of Defendant's failure to protect the personal information of Plaintiff and the Class; and

f. Whether Plaintiff and Class members have sustained damages, and if so, what is the proper measure of those damages.

47. Plaintiff's claims are typical of the claims of the respective Class he seeks to represent, because the Sensitive Information of Plaintiff, like the Sensitive Information of all Class members, was improperly accessed and/or misused by unauthorized persons.

48. Plaintiff will fairly and adequately represent and protect the interests of the Class, in that he has no interests that are antagonistic to or that irreconcilably conflict with those of other Class members.

49. Plaintiff has retained counsel competent and experienced in the prosecution of class action litigation.

50. A class action is superior to all other available methods for the fair and efficient adjudication of Plaintiff's and Class members' claims. Plaintiff and Class members have suffered harm as a result of Defendant's conduct. Certification of a class action to resolve these disputes will reduce the possibility of repetitious litigation involving hundreds of thousands of Class members. Further, certification is appropriate under Fed. R. Civ. P. 23, as the Class satisfies the requirements of Fed. R. Civ. P. 23(a) and 23(b)(3).

COUNT I
NEGLIGENCE

51. Plaintiff repeats and re-alleges all preceding allegations as if fully set forth herein.

52. Defendant requested and came into possession of Plaintiff's and Class members' Sensitive Information, and had a duty to exercise reasonable care in safeguarding and protecting such information from being accessed. Defendant's duty arose from, *inter alia*, the relationship between the parties, and from Aetna's own Privacy Policy.

53. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class members' Sensitive Information. The breach of security, unauthorized access, and resulting harm to Plaintiff and the Class were reasonably foreseeable to Defendant, particularly in light of its inadequate data security system and a prior data breach at Aetna in 2006.

54. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class members' Sensitive Information within Defendant's control.

55. Defendant, through its actions and/or omissions, breached its duty to Plaintiff and Class members by failing to have procedures in place to detect and prevent access to Plaintiff's and Class members' Sensitive Information by unauthorized persons.

56. Defendant also retained Class members' Sensitive Information for longer than necessary.

57. But for Defendant's breach of its duties, Plaintiff's and Class members' Sensitive Information would not have been compromised.

58. Plaintiff's and Class members' Sensitive Information was accessed as the proximate result of Defendant failing to exercise reasonable care in safeguarding such information by adopting, implementing, or maintaining appropriate security measures.

59. Defendant also had a duty to timely disclose to Plaintiff and Class members that their Sensitive Information had been, or was reasonably believed to have been, compromised. This duty arose from, *inter alia*, the relationship between the parties, and state notification statutes requiring timely notification of data breaches. Defendant failed to notify Class members

in a timely manner, waiting at least three weeks to contact 65,000 current and former employees, and never contacting the remainder of the 450,000 individuals affected by the breach.

60. Aetna's failure to comply with state notification statutes constituted *negligence per se*, satisfying the duty and breach elements of the negligence claim.

61. But for Defendant's breach of its duty to timely notify Class members, Class members would have had more time to scrutinize phishing email messages or otherwise protect themselves from the data breach.

62. Plaintiff and Class members suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; anxiety; emotional distress; loss of privacy; and other economic and non-economic harm.

COUNT II
BREACH OF IMPLIED CONTRACT

63. Plaintiff repeats and re-alleges all preceding allegations as if fully set forth herein.

64. Defendant requested and came into possession of Plaintiff's and Class members' Sensitive Information and had implied contracts with Plaintiff and Class members to protect such information, by way of Plaintiff and Class members providing Defendant with the requisite employment information.

65. The implied contracts arose from the course of conduct between Class members and Defendant, and Defendant's Privacy Policy provisions on its website.

66. The implied contracts required Defendant not to disclose Plaintiff's and Class

members' Sensitive Information to unauthorized third parties, and to safeguard the information from being accessed.

67. Defendant did not safeguard Plaintiff's and Class members' Sensitive Information from being accessed.

68. Because Defendant allowed unauthorized access to Plaintiff's and Class members' Sensitive Information and failed to safeguard the Sensitive Information, Defendant breached its implied contracts with Plaintiff and Class members.

69. A meeting of the minds occurred, as Plaintiff and Class members agreed to provide their Sensitive Information to Aetna in exchange for Aetna's agreement to, among other things, evaluate their applications and protect their Sensitive Information.

70. Plaintiff and Class members suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; anxiety; emotional distress; loss of privacy; and other economic and non-economic harm.

COUNT III
BREACH OF EXPRESS CONTRACT

71. Plaintiff repeats and re-alleges all preceding allegations as if fully set forth herein.

72. In exchange for Plaintiff and the Class applying for employment and providing Defendant with Sensitive Information as part of their applications, Defendant agreed to consider their applications and properly protect their Sensitive Information.

73. Aetna's express promise to safeguard Sensitive Information is contained in the

Privacy Policy provisions on its website.

74. The contracts required Defendant not to disclose Plaintiff's and Class members' Sensitive Information to unauthorized third parties, and to safeguard the information from being accessed.

75. Defendant did not safeguard Plaintiff's and Class members' Sensitive Information.

76. Because Defendant allowed unauthorized access to Plaintiff's and Class members' Sensitive Information and failed to safeguard the Sensitive Information, Defendant breached its contracts with Plaintiff and Class members.

77. A meeting of the minds occurred, as Plaintiff and Class members agreed to provide their Sensitive Information to Aetna in exchange for Aetna's agreement to, among other things, evaluate their applications and protect their Sensitive Information.

78. Plaintiff and Class members suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; anxiety; emotional distress; loss of privacy; and other economic and non-economic harm.

COUNT IV
NEGLIGENT MISREPRESENTATION

79. Plaintiff re-alleges all preceding allegations as if fully set forth herein.

80. When requesting information from Plaintiff and the Class in connection with their job applications, Aetna made various affirmative misrepresentations on its website regarding its

safeguarding of such information.

81. Aetna's statements regarding data security were material to Plaintiff and the Class because the statements provided assurance that the Sensitive Information would be protected.

82. Aetna made these misrepresentations while maintaining an inadequate security system. Aetna knew or should have known that its statements were inaccurate.

83. Aetna included the statements in its Privacy Policy in order to induce Plaintiff and the Class to submit their Sensitive Information.

84. In reliance on the misrepresentations, Plaintiff and the Class provided Aetna with their Sensitive Information.

85. The Sensitive Information was compromised, thereby causing damage to Plaintiff and the Class.

86. Plaintiff and Class members suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; anxiety; emotional distress; loss of privacy; and other economic and non-economic harm.

COUNT V
INVASION OF PRIVACY

87. Plaintiff re-alleges all preceding allegations as if fully set forth herein.

88. There are four theories for invasion of privacy: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of the others' name or likeness; (3) unreasonable publicity given to another's private life; and (4) publicity that unreasonably places the other in a

false light before the public.

89. Plaintiff asserts theories (1) and (3) here against Defendant.

90. Theory (1) does not require that the information be made public. Theory (3) does not require intentional conduct.

91. Plaintiff and Class members have a legally-protected privacy interest in their Sensitive Information, and a reasonable expectation of privacy in such information. This right of privacy includes the right not to have someone else misappropriate and misuse such information.

92. As a result of Defendant's unlawful actions, unauthorized intrusions were made into Plaintiff's and Class members' privacy when their Sensitive Information was accessed and/or misused without their knowledge, authorization, or consent. This unauthorized access and/or misuse is one that is highly offensive or objectionable to a reasonable person, including Plaintiff. Moreover, the disclosure of such private information, as alleged herein, does not include information that is of a legitimate public concern.

93. Defendant violated the rights of privacy of Plaintiff and Class members by allowing the access and/or misuse of their Sensitive Information without their consent.

94. On information and belief, the Sensitive Information of Plaintiff and the Class was obtained and disseminated to others for improper purposes.

95. As a result of Defendant's conduct, the privacy rights of Plaintiff and Class members have been violated, and Plaintiff and Class members have been harmed.

96. Plaintiff and Class members suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports;

time spent initiating fraud alerts; anxiety; emotional distress; loss of privacy; and other economic and non-economic harm.

JURY TRIAL DEMANDED

97. Plaintiff hereby demands a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, respectfully requests that the Court enter an Order:

a. Certifying the proposed Class under Fed. R. Civ. P. 23(a) and (b)(3) and appointing Plaintiff and Plaintiff's counsel to represent the Class;

b. Finding that Defendant is liable under all legal claims asserted herein for its failure to safeguard Plaintiff's and Class members' Sensitive Information;

c. Enjoining Defendant from actions which place Class members at a risk of future security breaches;

d. Awarding injunctive relief, including but not limited to: (i) the provision of identity theft protection services; (ii) the provision of appropriate credit monitoring services; (iii) the provision of identity theft insurance; and (iv) the requirement that Defendant receive periodic reviews by a qualified third party regarding the security of its computer systems used for storing employee and job applicant data;

e. Awarding compensation to Plaintiff and the Class as a result of the unauthorized access to their Sensitive Information;

f. Awarding damages to Plaintiff and the Class under the common law theories alleged herein;

g. Awarding punitive and/or treble damages as provided under relevant laws;

h. Awarding all costs, including attorneys' fees, and the costs of prosecuting this action;

i. Awarding pre and post judgment interest as prescribed by law; and

j. Awarding any other legal or equitable relief as justice requires.

Respectfully submitted,

Dated: July 30, 2009 BERGER & MONTAGUE, P.C.

By s/ Sherrie R. Savett

Sherrie R. Savett, Esq. (Pa. I.D. No.17646)
Michael T. Fantini, Esq. (Pa. I.D. No. 57192)
Jon Lambiras, Esq. (Pa. I.D. No.92384)
1622 Locust Street
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4636

SHELLER, P.C.
Jamie L. Sheller, Esq. (Pa. I.D. No. 55722)
1528 Walnut Street, 3rd Floor
Philadelphia, PA 19102
Tel: (215) 790-7300
Fax: (215) 546-0942

Counsel for Plaintiff and the Class

Exhibit 1

Elease Wright
Human Resources
151 Farmington Avenue
Hartford, CT 06156

July 16, 2009

Cornelius J Allison
212 S 7TH ST
Darby, Pennsylvania 19023-2430

Dear Cornelius:

Your Credit Monitoring Promotion Code: **304091763877**

We recently learned that e-mail addresses were accessed from a web site and database hosted by an external vendor to manage job applications for current or previous Aetna employees. Because other personal information about current or previous Aetna employees is included in this same database, it is possible that other personal information may have been exposed. Once we discovered the potential exposure, we immediately initiated a thorough review of the database and its security environment and instituted additional protective measures. Although we have been unable to determine how these e-mail addresses were acquired by the third party, we continue to work with the vendor and an IT security firm to ensure the security of the information stored in this database.

While we are not able to verify whether your personal information was accessed, the database included information you provided as an employee with Aetna. This information included your name, address, Social Security Number (SSN), date of birth, phone number, e-mail address and information pertaining to prior jobs. The data did not include any banking, financial or health information.

We take the confidentiality of personal information very seriously. That is why we have comprehensive policies and procedures in place to safeguard your privacy. We truly regret that in some isolated instances, however, errors do occur.

As a precautionary measure, we are offering credit monitoring assistance to you (see information following this letter). The service is available at no cost to you. To take advantage of this offer, you must contact Equifax within 90 days as detailed in the accompanying information. Use the Credit Monitoring Promotion Code at the top of this letter to enroll in the Equifax program.

Please know that Aetna is committed to protecting personal information, and we will continue to monitor, review and enhance our company's privacy procedures. We have taken appropriate action to ensure that our security procedures are followed. We apologize for any inconvenience or concern this situation may cause you. If you have any questions regarding this matter, you should call Aetna's Human Resource Contact Center at 1-800-238-6247 and select Option 6 to reach a customer service representative.

Sincerely,

Elease Wright
Senior Vice President

Steps to Take to Protect Your Identity

We urge you to monitor your personal accounts (e.g., bank statements, credit card bills, etc.) for charges or other items you do not recognize.

We also urge you to **place a fraud alert on your credit file.** A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may call any one of the three major credit reporting companies. As soon as one credit reporting company confirms your fraud alert, the other credit agencies are notified to place a similar alert. An initial fraud alert stays on your credit report for 90 days and is available without charge.

Here is how you can contact the major credit reporting companies. Again, you only need to contact one, and the others will be notified:

- Equifax: 1-877-478-7625; www.equifax.com; P.O. Box 740241, Atlanta, GA, 30374-0241
- Experian: 1-888-397-3742; www.experian.com, P.O. Box 9532, Allen, TX 75013
- TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Under federal law, you are entitled to a free copy of your credit report, at your request, from each of the major nationwide credit reporting companies once every 12 months. To order your free annual credit report from one or all of the national credit reporting companies, visit www.annualcreditreport.com, call toll free 1-877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print the form from www.ftc.gov/credit.

Once you receive your reports, **review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain.** Verify the accuracy of your Social Security Number, address(es), complete name and employer(s). Notify the credit reporting companies if any information is incorrect.

Additional Credit Monitoring Assistance

In addition, we have arranged with Equifax Personal Solutions to help you protect your identity and your credit information at no cost to you. To take advantage of this offer, you must contact Equifax within 90 days of the date of this letter.

The steps to follow are:

1. Enroll in Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection service. This product is being provided to you at no cost.
2. Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at Equifax and the other two credit reporting agencies

Enroll in Equifax Credit Watch™ Gold with 3-in-1 Monitoring

Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit reporting agencies. The key features and benefits are listed below.

Equifax Credit Watch provides you with a 1 year membership service:

- Comprehensive credit file monitoring of your Equifax, Experian, and TransUnion credit reports with daily notification of key changes to your credit files from any of the three agencies.
- Wireless alerts and customizable alerts available
- One 3-in-1 Credit Report and unlimited access to your Equifax Credit Report™
- $1 million in identity theft insurance with $0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and to investigate inaccurate information.

How to Enroll On Line

Equifax has a simple Internet-based verification and enrollment process.

Visit: www.myservices.equifax.com/tri

1. Consumer Information: complete the form with your contact information (name, address and e-mail address) and click "Continue" button. The information is provided in a secured environment.
2. Identity Verification: complete the form with your Social Security Number, date of birth and telephone # s; create a User Name and Password; agree to the Terms of Use; and click "Continue" button. The system will ask you up to two security questions to verify your identity.
3. Payment Information: During the "check out" process, provide the promotional code that is printed at the top of the accompanying letter in the "Enter Promotion Code" box (no spaces, include dash). After entering your code press the "Apply Code" button and then the "Submit Order" button at the bottom of the page. (This code eliminates the need to provide a credit card number for payment.)
4. Order Confirmation: – Click "View My Product" to access your 3-in-1 Credit Report and other product features.

How to Enroll By Mail

To sign up for US Mail delivery of the product, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Promotion Code: You will be asked to enter your promotion code that is printed at the top of the accompanying letter (no spaces, **no dash**)
2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax can not process your enrollment.
4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided).

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your Equifax credit file, you may contact Equifax' auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

You can find further general information about identity theft by accessing the:

- U.S. Federal Trade Commission site at http://www.consumer.gov/idtheft/con_pubs.htm
- Federal Trade Commission site at http://www.consumer.gov/idtheft/con_steps.htm

† Identity Fraud Expense Reimbursement Master Policy underwritten by Travelers Casualty and Surety Company of America and its property casualty affiliates, Hartford, CT 06183. Coverage for all claims or losses depends on actual policy provisions. Availability of coverage can depend on Equifax underwriting qualifications and state regulations. Coverage not available for residents of New York.

CERTIFICATE OF SERVICE

I hereby certify that on July 30, 2009, the foregoing Amended Class Action Complaint was served via U.S. mail on the following:

ELLIOTT GREENLEAF & SIEDZIKOWSKI, P.C.
John M. Elliott
Mark J. Schwemler
Timothy T. Myers
Stewart J. Greenleaf, Jr.
925 Harvest Drive, Suite 300
Blue Bell, PA 19422
Tel: (215) 977-1000

Counsel for Defendant

By: s/ Jon Lambiras
Jon Lambiras

malta500244-006